Priority is claimed from:

Country	Application No	Filing Date
Europe	02360235.2	August 8, 2002

The priority document is enclosed herewith.

Respectfully submitted,
SUGHRUE MION, PLLC

Attorneys for Applicant

By: _____
Brian W. Hannon
Registration No. 32,778
for David J. Cushing
Registration No. 28,703

SUGHRUE MION, PLLC
Telephone: (202) 293-7060
Facsimile: (202) 293-7860

WASHINGTON OFFICE
23373
CUSTOMER NUMBER

P.B.5818 – Patentlaan 2
2280 HV Rijswijk (ZH)
☎ +31 70 340 2040
TX 31651 epo nl
FAX +31 70 340 3016

Europäisch s Patentamt
Zweigstelle in Den Haag Recherchen–abteilung

European Patent Offic
Branch at The Hague Search division

Office européen des br vets
Département à La Haye Division de la recherche

Menzietti, Domenico, Dipl.-Ing
Alcatel
Intellectual Property Department, Stuttgart
70430 Stuttgart
ALLEMAGNE

Eingang bei ZPL
27. JAN. 2003
Term. Bearb. 27. 03. 03

Eing...
27.
Term. Bearb.

Datum/Date
28.01.03

Zeichen/Ref./Réf.	Anmeldung Nr./Application No./Demande n°./Patent Nr./Patent No./Brevet n°.
113 586	02360235.2-1244-

Anmelder/Applicant/Demandeur/Patentinhaber/Proprietor/Titulaire
ALCATEL

Weiter mit A1-3

17.3.03

COMMUNICATION

The European Patent Office herewith transmits as an enclosure the European search report for the above–mentioned European patent application.

If applicable, copies of the documents cited in the European search report are attached.

☐ Additional set(s) of copies of the documents cited in the European search report is (are) enclosed as well.

The following specifications given by the applicant have been approved by the Search Division:

☒ abstract ☒ title

☐ The abstract was modified by the Search Division and the definitive text is attached to this communication.

The following figure will be published together with the abstract: 2

EUROPÄISCHES PATENTAMT - EUROPEAN PATENT OFFICE - OFFICE EUROPÉEN DES BREVETS - DEN HAAG - THE HAGUE - LA HAYE

REFUND OF THE SEARCH FEE

If applicable under Article 10 Rules relating to fees, a separate communication from the Receiving Section on the refund of the search fee will be sent later.

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 02 36 0235

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
X	THERNELIUS F: "SIP, NAT, and Firewalls" MASTER'S THESIS, KUNGST TEKNISKA HÖGSKOLAN, DEPARTMENT OF TELEINFORMATICS - ERICSSON, May 2000 (2000-05), XP002209773 * page 14; figure 11 * * page 31, line 36 - line 48; figure 32 * * page 33, line 1 - page 34, line 33; table 5 *	4-7	H04L29/06 H04M7/00
X	WO 02 15627 A (PARANTAINEN JANNE ;EINOLA HEIKKI (FI); HAMITI SHKUMBIN (FI); HURTT) 21 February 2002 (2002-02-21) * page 14, line 7 - page 15, line 31 *	4,7	
A	EP 1 111 892 A (NORTEL NETWORKS LTD) 27 June 2001 (2001-06-27) * abstract * * page 4, column 5, paragraph 18 - page 5, column 7, paragraph 25 * * page 9, column 16, paragraph 57 - page 11, column 19, line 11 *	1-7	TECHNICAL FIELDS SEARCHED (Int.Cl.7) H04L H04M H04Q
A	WO 01 89145 A (ERICSSON TELEFON AB L M) 22 November 2001 (2001-11-22) * abstract * * page 3, line 20 - page 4, line 2 * * page 4, line 27 - page 5, line 2 * * page 6, line 10 - page 7, line 27 *	1-7	
A	WO 99 17499 A (NOKIA TELECOMMUNICATIONS OY ;HAUMONT SERGE (FI)) 8 April 1999 (1999-04-08) * page 9, line 18 - line 31 * * abstract * * page 10, line 9 - line 29 * * claims 1,3,4,7-9 *	1-7	

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	16 January 2003	Karavassilis, N

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

1

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 02 36 0235

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

16-01-2003

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0215627 A	21-02-2002	WO 0215625 A1	21-02-2002
		AU 6701800 A	25-02-2002
		AU 8767601 A	25-02-2002
		WO 0215627 A1	21-02-2002
EP 1111892 A	27-06-2001	EP 1111892 A2	27-06-2001
WO 0189145 A	22-11-2001	AU 5690501 A	26-11-2001
		WO 0189145 A2	22-11-2001
WO 9917499 A	08-04-1999	FI 973806 A	27-03-1999
		AU 9351598 A	23-04-1999
		CA 2304172 A1	08-04-1999
		CN 1277771 T	20-12-2000
		EP 1018241 A2	12-07-2000
		WO 9917499 A2	08-04-1999
		JP 2001518744 T	16-10-2001
		TW 429710 B	11-04-2001

Eur päisches Patentamt | European Patent Office | Office européen des brevets

Bescheinigung | Certificate | Attestation

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.

The attached documents are exact copies of the European patent application described on the following page, as originally filed.

Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet européen spécifiée à la page suivante.

Patentanmeldung Nr. | Patent application No. | Demande de brevet n°

02360235.2

Der Präsident des Europäischen Patentamts;
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

R C van Dijk

DEN HAAG, DEN
THE HAGUE, 06/09/02
LA HAYE, LE

Europäisches Patentamt | European Patent Office | Office eur péen des brevets

Blatt 2 der Bescheinigung
Sheet 2 of the certificate
Page 2 de l'attestation

Anmeldung Nr.:
Application no.: 02360235.2
Demande n°:

Anmeldetag:
Date of filing: 08/08/02
Date de dépôt:

Anmelder:
Applicant(s):
Demandeur(s):
ALCATEL
75008 Paris
FRANCE

Bezeichnung der Erfindung:
Title of the invention:
Titre de l'invention:
Lawful interception for VoIP calls in IP based networks

In Anspruch genommene Priorität(en) / Priority(ies) claimed / Priorité(s) revendiquée(s)

Staat: State: Pays:	Tag: Date: Date:	Aktenzeichen: File no. Numéro de dépôt:

Internationale Patentklassifikation:
International Patent classification:
Classification internationale des brevets:
/

Am Anmeldetag benannte Vertragstaaten:
Contracting states designated at date of filing: AT/BE/CH/CY/DE/DK/ES/FI/FR/GB/GR/IE/IT/LI/LU/MC/NL/PT/SE/TR
Etats contractants désignés lors du depôt:

Bemerkungen:
Remarks:
Remarques:

Lawful interception for VoIP calls in IP based networks

TECHNICAL FIELD OF THE INVENTION

This invention is related in general to the field of telecommunications systems. More particularly, the invention is related to a lawful interception device for media streams, in particular VoIP calls in IP based networks.

BACKGROUND OF THE INVENTION

Current lawful interceptions are deployed in class4/class5 switches of PSTN/PLMN networks. In 3G/UMTS or next generation networks, a connection may be IP end to end. No traffics will go through class 5/class4 switches. That means current lawful interception solutions cannot be used here. One solution may undertake an analysis of IP packets in a related network node, but it's difficult to know which route a call (media stream) will take through the network.

SUMMARY OF THE INVENTION

It is an object of the invention to provide a lawful interception device for VoIP calls in IP based networks.

The inventive lawful interception device detects information in the signalling information being transmitted between two IP parties and generates instructions out of the detected signalling information for instructing a RTP (Real-time Transport Protocol) proxy server to create channels to bypass a VoIP call to be intercepted via an intermediate storage medium. Instead of voice each media stream could be intercepted, e.g. data, internet access, e-mail, video, real-time pictures, etc.

In a SIP (Session Initiation Protocol) interception proxy server, where interception should be controlled, applications for interception are running to chose calls for interception. If a call should be monitored, the SIP proxy server has first to hold the invite message from A party. There are listening information in SDP (session description protocol) part of invite message.

SIP proxy server then instructs a RTP proxy server via a RTP proxy control interface to allocate a bypass channel for monitoring the media stream (A channel: sending to A party). The RTP information of this bypass channel (listening part: ip and port) is included in SDP part in the SIP invite message and passed to its destination.

When SIP proxy server has received a response of B party, he instructs RTP proxy via RTP proxy control interface to allocate another bypass channel for monitoring the media stream (B channel: sending to B party). The RTP information of this second bypass channel (listening part: ip and port) is included in SDP part in SIP ok message and send to its origination (A party).

After session setup, both parties will start RTP connections to RTP proxy server depending on connection parameters in its received SIP messages. But those are transparent to A and B. They do not know they are connected to a RTP proxy.

The RTP proxy can start record both media channels (A and B). At the end of this call, e.g. a media file with two sound tracks will be created by RTP proxy.

Advantages:

- centralized network node to intercept media streams,
- low cost of deployment,
- transparent to end users,
- the RTP proxy can also be used in the same way as above in a media gateway control (MEGACO, H.248) based network or H.323 network.

BRIEF DESCRIPTION OF THE DRAWINGS

For a better understanding of the present invention, reference is made to the accompanying drawings, in which:

FIG. 1 is a simplified block diagram of a portion of an exemplary telecommunications network according to the teachings of the prior art;

FIG. 2 is a simplified block diagram of a portion of an exemplary telecommunications network according to the teachings of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

FIG. 1 shows a portion of an exemplary telecommunications network according to the teachings of the prior art.

Two IP parties, e.g. yshen@alcatel.de and eric@alcatel.com, are interconnected via two networks: a SIP signaling network and a transmission network. Via the SIP signaling network signaling is performed, e.g. a connection is established between the two IP parties. Via the

transmission network the information to be transmitted, e.g. voice, data, etc. is transmitted in media streams (RTP session).

In the SIP based network, each SIP proxy server is responsible for signaling and session monitoring. The media stream will go from one IP endpoint to another IP endpoint. There is no need of a centralized media path like in PSTN network. A lawful interception of media stream could be done only in the network layer.

Recording media stream by analyzing network traffics for lawful interception is very expensive, due to the packet route through the IP network could change. Therefor the recording could only be done very closely to the endpoints. Additionaly a resembling of recorded packets is needed. A playing in real time will be difficult.

In the following definition and background information is provided regarding SIP, proxy server, RTP, SDP, etc.

SIP:

The Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol for creating, modifying and terminating sessions with one or more participants. These sessions include Internet multimedia conferences, Internet telephone calls and multimedia distribution. Members in a session can communicate via multicast or via a mesh of unicast relations, or a combination of these.

SIP invitations used to create sessions carry session descriptions which allow participants to agree on a set of compatible media types. SIP supports user mobility by proxying and redirecting requests to the user's current location. Users can register their current location. SIP is not tied to any particular conference control protocol. SIP is designed to be independent of the lower-layer transport protocol and can be extended with additional capabilities.

The Session Initiation Protocol (SIP) is an application-layer control protocol that can establish, modify and terminate multimedia sessions or calls. These multimedia sessions include multimedia conferences, distance learning, Internet telephony and similar applications. SIP can invite both persons and "robots", such as a media storage service. SIP can invite parties to both unicast and multicast sessions; the initiator does not necessarily have to be a member of the session to which it is inviting. Media and participants can be added to an existing session.

SIP can be used to initiate sessions as well as invite members to sessions that have been advertised and established by other means. Sessions can be advertised using multicast protocols such as electronic mail, news groups, web pages or directories (LDAP), among others.

SIP transparently supports name mapping and redirection services, allowing the implementation of ISDN and Intelligent Network telephony subscriber services. These facilities also enable personal mobility. In the parlance of telecommunications intelligent network services, this is defined as: "Personal mobility is the ability of end users to originate and receive calls and access subscribed telecommunication services on any terminal in any location, and the ability of the network to identify end users as they move. Personal mobility is based on the use of a unique personal identity (i.e., personal number)." Personal mobility complements terminal mobility, i.e., the ability to maintain communications when moving a single end system from one subnet to another.

SIP supports five facets of establishing and terminating multimedia communications:

User location: determination of the end system to be used for

communication;

User capabilities: determination of the media and media parameters to be used;

User availability: determination of the willingness of the called party to engage in communications;

Call setup: "ringing", establishment of call parameters at both called and calling party;

Call handling: including transfer and termination of calls.

SIP can also initiate multi-party calls using a multipoint control unit (MCU) or fully-meshed interconnection instead of multicast. Internet telephony gateways that connect Public Switched Telephone Network (PSTN) parties can also use SIP to set up calls between them.

SIP is designed as part of the overall IETF multimedia data and control architecture currently incorporating protocols such as the real-time transport protocol (RTP) for transporting real-time data and providing QoS feedback.

A request and a response form together a transaction. SIP uses e.g. invite and ack messages to build up connections. Other messages used are e.g. ok, bye, options, register, cancel. SIP parties are identified via a SIP-ULR, e.g.: sip:clientname@hostaddress. Each client may transmit requests to a proxy server or directly to an IP address.

An establishment of a connection is perfomed is three steps: sending an invite (request) message from a first IP party to a second IP party, sending an ok (response) message from the second IP party to the first IP party, sending an ack (response) message from the frist IP party to the second IP party. The invite message includes as much information as needed to allow

the second IP party to judge whether a connection is wanted or not. The ack message is an acknowledgement, which serves to increase savety of the connection. SIP is thus not dependent on TCP or UDP.

The SIP according to the invention is the SIP currently standardized and modifications thereof and equivalents thereof.

RTP:

The Audio/Video Transport Working Group of IETF was formed to specify a protocol for real-time transmission of audio and video over UDP and IP multicast. This is the Real-time Transport Protocol, RTP, together with its associated profile for audio/video conferences and payload format documents. The payload formats currently under discussion include a number of media specific formats (MPEG-4, DTMF, PureVoice) and FEC techniques applicable to multiple formats (parity FEC, Reed-Solomon coding). RTP is used to replace a normal circuit-switched trunk between two nodes.

The real-time transport protocol (RTP) is a payload format to be used for e.g. Adaptive Multi-Rate (AMR) and Adaptive Multi-Rate Wideband (AMR-WB) encoded speech signals. RTP provides end-to-end network transport functions suitable for applications transmitting real-time data, such as audio, video or simulation data, over multicast or unicast network services. RTP does not address resource reservation and does not guarantee quality-of service for real-time services. The data transport is e.g. augmented by the control protocol RTCP (Real-time Transport Control Protocol) to allow monitoring of the data delivery in a manner scalable to large multicast networks, and to provide minimal control and identification functionality. RTP and RTCP are designed to be independent of the underlying transport and network layers. The protocol supports the use of RTP-level translators and mixers. The data transported by RTP in a packet, for example audio samples or compressed video data. A data packet includes e.g. the fixed

RTP header, a possibly empty list of contributing sources, and the payload data.

The RTP according to the invention is the RTP currently under discussion and modifications thereof and equivalents thereof. RTP may be a protocol for both audio and video, or audio only, or video only, or audio, video and data, or audio and data, etc. One modification of RTP is e.g. RTP/I, an application level real-time protocol for distributed interactive media. Typical examples of distributed interactive media are shared whiteboards, networked computer games and distributed virtual environments. RTP/I defines a standardized framing for the transmission of data and provides mechanisms that are universally needed for this media class. Thereby RTP/I enables the development of reusable functionality and generic services that can be employed for multiple distributed interactive media. Examples for this kind of functionality are the ability to record sessions, to support late coming participants, and to provide security services. RTP/I is a protocol that follows the ideas of application level framing and integrated layer processing. It has been designed to be independent of the underlying network and transport layers. Thus RTP/I as a modified RTP protocol that reuses many aspects of RTP while it is thoroughly adapted to the specific needs of distributed interactive media.

Proxy, proxy server:

An intermediary program that acts as both a server and a client for the purpose of making requests on behalf of other clients. Requests are serviced internally or by passing them on, possibly after translation, to other servers. A proxy interprets, and, if necessary, rewrites a request message before forwarding it.

Server:

A server is an application program that accepts requests in order to service requests and sends back responses to those requests. Servers are either proxy, redirect or user agent servers or registrars.

User agent client (UAC), calling user agent:

A user agent client is a client application that initiates the SIP request.

SDP:

The Session Description Protocol (SDP) is intended for describing multimedia sessions for the purposes of session announcement, session invitation, and other forms of multimedia session initiation.

The purpose of SDP is to convey information about media streams in multimedia sessions to allow the recipients of a session description to participate in the session. SDP is primarily intended for use in an internetwork, although it is sufficiently general that it can describe conferences in other network environments.

A multimedia session, for these purposes, is defined as a set of media streams that exist for some duration of time. Media streams can be many-to-many. The times during which the session is active need not be continuous.

Thus far, multicast based sessions on the Internet have differed from many other forms of conferencing in that anyone receiving the traffic can join the session (unless the session traffic is encrypted). In such an environment, SDP serves two primary purposes. It is a means to communicate the existence of a session, and is a means to convey sufficient information to enable joining and participating in the session. In a unicast environment, only the latter purpose is likely to be relevant.

Thus SDP includes:

o Session name and purpose
o Time(s) the session is active
o The media comprising the session
o Information to receive those media (addresses, ports, formats and so on)

As resources necessary to participate in a session may be limited, some additional information may also be desirable:

o Information about the bandwidth to be used by the conference
o Contact information for the person responsible for the session

In general, SDP must convey sufficient information to be able to join a session (with the possible exception of encryption keys) and to announce the resources to be used to non-participants that may need to know.

SDP includes:

o The type of media (video, audio, etc)
o The transport protocol (RTP/UDP/IP, H.320, etc)
o The format of the media (H.261 video, MPEG video, etc)

For an IP multicast session, the following are also conveyed:

o Multicast address for media
o Transport Port for media

This address and port are the destination address and destination port of the multicast stream, whether being sent, received, or both.

For an IP unicast session, the following are conveyed:

o Remote address for media
o Transport port for contact address

The semantics of this address and port depend on the media and transport protocol defined. By default, this is the remote address and remote port to which data is sent, and the remote address and local port on which to receive data. However, some media may define to use these to establish a control channel for the actual media flow.

The SDP according to the invention is the SDP currently standardized and modifications thereof and equivalents thereof.

FIG. 2 shows a portion of an exemplary telecommunications network according to the teachings of the present invention.

Like in fig. 1 two IP parties, e.g. yshen@alcatel.de and eric@alcatel.com, are interconnected via two networks: a SIP signaling network and a transmission network. Via the SIP signaling network signaling is performed, e.g. a connection is established between the two IP parties. Via the transmission network the information to be transmitted, e.g. voice, data, etc. is transmitted in media streams (RTP session).

Different from fig. 1 a lawful interception device is included in fig. 2. The lawful interception device is e.g. a processor with particular software. The processor is e.g. a digital signal processor, a controller, a microprocessor or the like. Instead of one processor two or more processors could be used. Two or more processors could be located at different sites. One processor could be used to perform SIP proxy server operations and another processor could be used to perform RTP proxy server operations. In general, one, two or more hardwares could be used to run one, two, or

more softwares. Each software could in addition be run in parts on different hardware.

The lawful interception device includes a SIP (Session Initiation Protocol) proxy server or a MGC (Media Gateway Controller) to detect information in the signalling information being transmitted between two IP (Internet Protocol) parties and to generate instructions out of the detected signalling information for instructing a RTP (Real-time Transport Protocol) proxy server to create channels to bypass a media stream to be intercepted via an intermediate storage medium. Media streams are e.g. VoIP, data, internet access, e-mail, video, real-time pictures, music, video clips, video games, etc. The storage medium could be a compact disk, a magnetic storage medium, a read access memory, or the like.

The method for performing SIP signaling for a media stream includes the following steps:

receiving a SIP invite message of a first IP party,

adapting at least one connection parameter in the SDP (Session Description Protocol) of the received SIP invite message,

transmitting the adapted SIP invite message to a second IP party,

receiving a SIP response message of the seond IP party,

adapting at least one connection parameter in the SDP (Session Description Protocol) of the received SIP response message,

transmitting the adapted SIP response message to the first IP party.

At least one RTP parameter includes information about a bypass channel, an address, or a port. The RTP parameters sent to both IP parties differ from each other.

After receipt of the SIP invite message of the first IP party the SIP interception proxy server sends a request to the RTP interception proxy server to assign at least two channels for bothway communication. The interface used to communicate between SIP interception proxy server and RTP interception proxy server is a XML based API. The number of channels to be assigned may vary dependent of the amount of data to be transmitted, of the bandwith requested, of the quality of service requested, of the kind of information to be transmitted, e.g. voice, voice and data, voice and video, etc. At least one channel is assigned to transmit information between the RTP interception proxy server and the terminal of the first IP party. The terminal could be a phone, a laptop, a personal computer, a screenphone, a mobile phone, etc. At least one other channel is assigned to transmit information between the RTP interception proxy server and the terminal of the second IP party.

Assume channel A at the RTP interception proxy server is assigned to transmit information between the second IP terminal and the terminal of the first IP party, and channel B is assigned to transmit information between the the terminal of the first IP party and the second IP terminal. Then the RTP interception proxy server sends information about the assignment of channels A and B to the SIP interception proxy server. The SIP interception proxy server includes information about channel A in the invite message to be send to the second IP party. The information about channel A is advantageously included in the connection parameter information to be included in the SDP of the SIP invite message.

After receipt of the SIP response message of the seond IP party, which corresponds to an ok message stating that a connection to the first IP party is desired, the SIP interception proxy server exchanges the connection parameter included in the SDP part of the ok message by the information about channel B. The modified ok message including the information about channel B is send to the first IP party.

Thus the first IP party will send data to channel B and receive data via channel A of the RTP interception proxy server. The second IP party will send data to channel A and receive data via channel B of the RTP interception proxy server. Within the lawful interception device the intermediate storage medium is connected to both channel A and B. Thus the information flow between both IP parties will transfer the intermediate storage medium and thus interception is enabled. The first party is not aware on which channel the second party is sending, and the second party is not aware on which channel the first party is sending. Thus interception is transparent regarding the two IP parties.

A computer program for performing at least part of the steps of the inventive method could be used as an upgrade software, which is sold e.g. to service providers, which will upgrade one or more SIP proxy server thus enabling a usual SIP proxy server having the functionality of an SIP interception proxy server. The computer program includes at least the following steps:

adapting at least one connection parameter in the SDP (Session Description Protocol) of the received SIP invite message,

adapting at least one connection parameter in the SDP (Session Description Protocol) of the received SIP response message.

The computer program could also be programmed to perform all steps of the method as described above.

Within an IP network one, two, or more SIP proxy servers could be used, one, two, or more SIP interception proxy servers could be used, one, two, or more RTP proxy servers could be used, and one, two, or more RTP interception proxy servers could be used.

The IP network could be a wireline network, a wireless network, or a combination of both.

List of abbreviations:

3G	Third Generation
API	Application Programmer Interface
AMR	Adaptive Multi-Rate
AMR-WB	AMR-Wideband
DTMF	Dual-Tone Multi-Frequency
FEC	Forward Error Correction
H248	ITU standard
H261	ITU standard
H320	ITU standard
H323	ITU standard
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISDN	Integrated Services Digital Network
LDAP	Lightweight Directory Access Protocol
MEGACO	Media Gateway Controller
MCU	Multipoint Control Unit
MPEG	Motion Picture Expert Group
MGC	Media Gateway Controller
NGN	Next Generation Network
PSTN	Public Switched Telephone Network
PLMN	Public Land Mobile Network
QoS	Quality of Service
RTCP	Real-time Transport Control Protocol
RTP	Real-time Transport Protocol
SDP	Session Description Protocol
SIP	Session Initiation Protocol
TCP	Transmission Control Protocol
UAC	User Agent Client
UDP	User Datagram Protocol
UMTS	Universal Mobile Transmission System
VoIP	Voice over IP
XML	eXtensible Markup Language

Claims

1. Lawful interception device including a SIP (Session Initiation Protocol) proxy server or a MGC (Media Gateway Controller) to detect information in the signalling information being transmitted between two IP (Internet Protocol) parties and to generate instructions out of the detected signalling information for instructing a RTP (Real-time Transport Protocol) proxy server to create channels to bypass a media stream to be intercepted via an intermediate storage medium.

2. SIP interception proxy server to detect information in the signalling information being transmitted between two IP (Internet Protocol) parties and to generate instructions out of the detected signalling information for instructing a RTP (Real-time Transport Protocol) proxy server to create channels to bypass a media stream to be intercepted via an intermediate storage medium.

3. Interception MGC to detect information in the signalling information being transmitted between two IP (Internet Protocol) parties and to generate instructions out of the detected signalling information for instructing a RTP (Real-time Transport Protocol) proxy server to create channels to bypass a media stream to be intercepted via an intermediate storage medium.

4. Method for performing SIP signaling for a media stream, including the following steps:

   receiving a SIP invite message of a first IP party,

   adapting at least one connection parameter in the SDP (Session Description Protocol) of the received SIP invite message,

   transmitting the adapted SIP invite message to a second IP party,

   receiving a SIP response message of the seond IP party,

   adapting at least one connection parameter in the SDP (Session Description Protocol) of the received SIP response message,

   transmitting the adapted SIP response message to the first IP party.

5. Method according to claim 4, wherein at least one connection parameter includes information about a bypass channel, an address, or a port.

6. Method according to claim 4, wherein the connection parameters sent to both IP parties differ from each other.

7. Computer program for performing at least part of the steps of the method according to claim 4, including the following steps:

   adapting at least one connection parameter in the SDP (Session Description Protocol) of the received SIP invite message,

   adapting at least one connection parameter in the SDP (Session Description Protocol) of the received SIP response message.

Abstract

Lawful interception for VoIP calls in IP based networks

The lawful interception device to monitor media streams of two IP parties includes a SIP (Session Initiation Protocol) proxy server or a MGC (Media Gateway Controller) to detect information in the signalling information being transmitted between the two IP (Internet Protocol) parties and to generate instructions out of the detected signalling information for instructing a RTP (Real-time Transport Protocol) proxy server to create channels to bypass a media stream to be intercepted via an intermediate storage medium. Due to adaptation of connection parameters in the SDP part of the SIP messages sent to the IP parties the interception is transparent to the IP parties.

(Fig. 2)

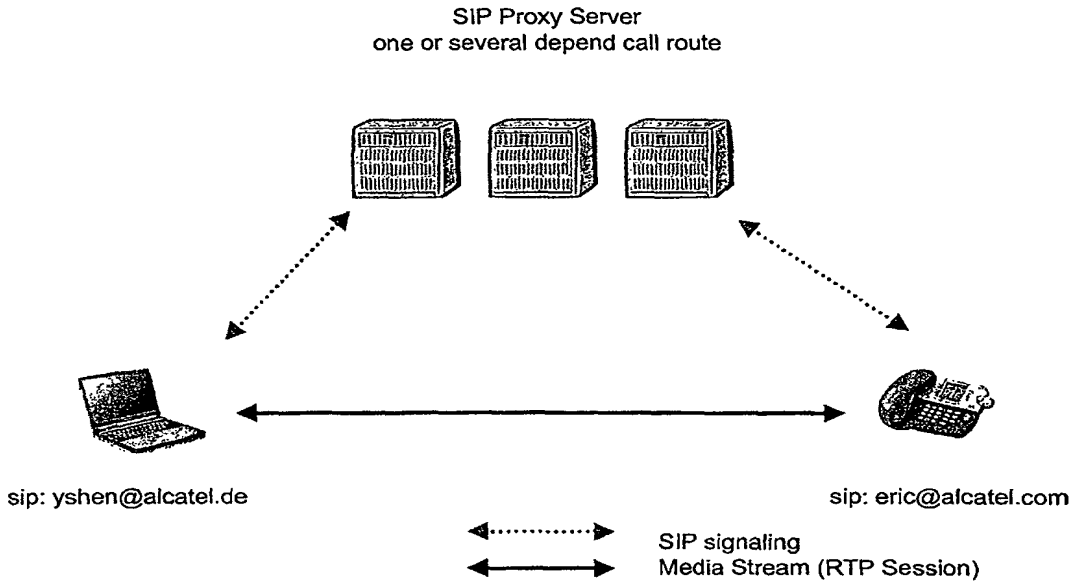
SIP Proxy Server
one or several depend call route
sip: yshen@alcatel.de
sip: eric@alcatel.com
SIP signaling
Media Stream (RTP Session)

Fig. 1

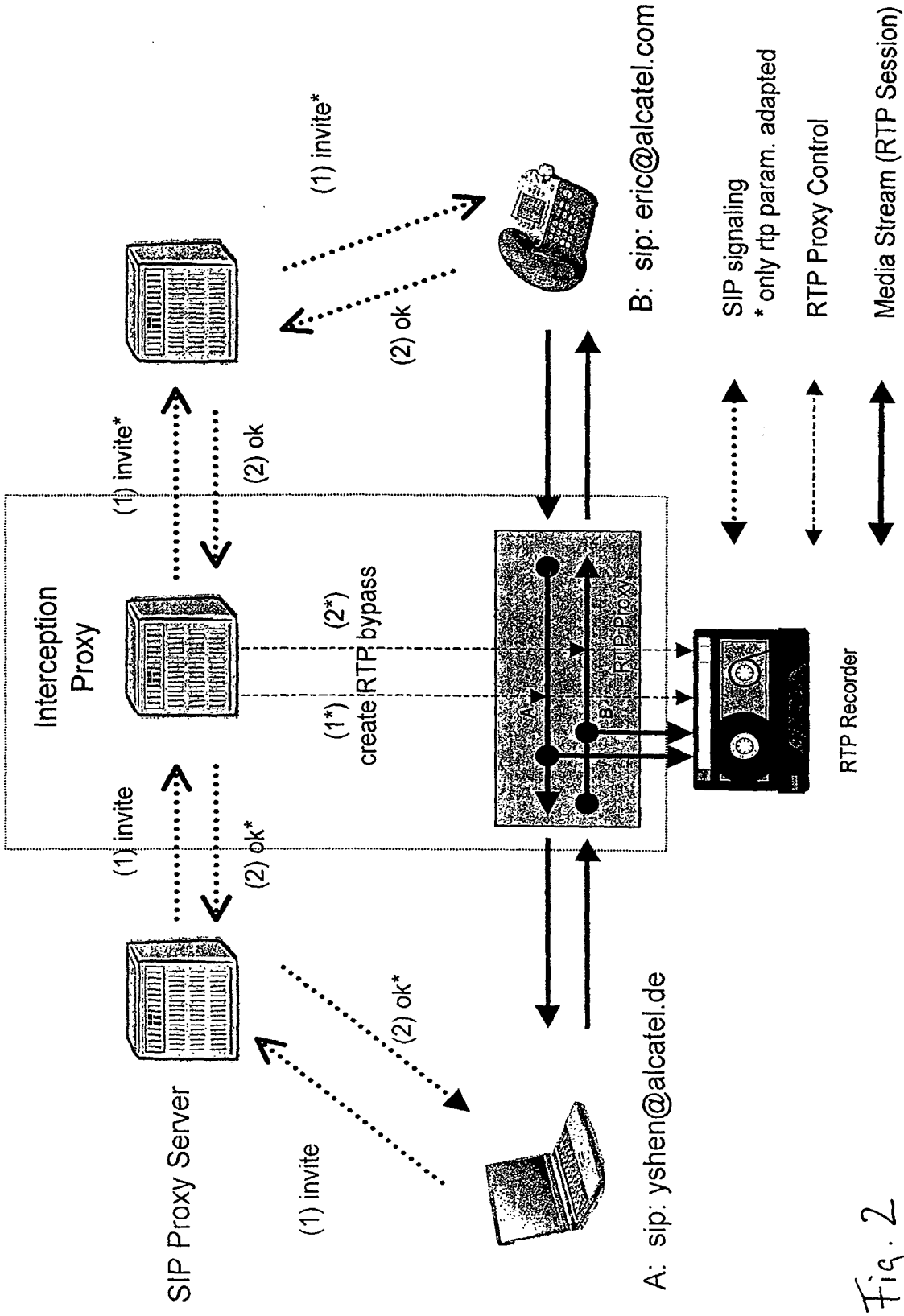
SIP Proxy Server
Interception Proxy
(1) invite
(2) ok*
(1) invite*
(2) ok
(1*) create
(2*) RTP bypass
(1) invite*
(2) ok
(1) invite
(2) ok*
A: sip: yshen@alcatel.de
B: sip: eric@alcatel.com
A'
B'
RTP Proxy
RTP Recorder
SIP signaling
* only rtp param. adapted
RTP Proxy Control
Media Stream (RTP Session)

Fig. 2